the President under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 *et seq.*) or to facilitate recovery from terrorism or nuclear, biological, chemical, or radiological attack.

(b) If the Schedule Contractor accepts an order from an entity identified in paragraph (d) of the clause at 552.238–78, Scope of Contract (Eligible Ordering Activities)—Alternate I, the Contractor agrees to the following conditions—

(1) The ordering activity is responsible for all payments due the Contractor for the contract formed by acceptance of the order, without recourse to the agency of the U.S. Government, which awarded the Schedule contract.

(2) The Contractor is encouraged, but not obligated, to accept orders from such entities. The Contractor may, within 5 days of receipt of the order, decline to accept any order, for any reason. The Contractor shall decline the order using the same means as those used to place the order. The Contractor shall fulfill orders placed by such entities, which are not declined within the 5-day period.

(c) In accordance with clause 552.238–74, Industrial Funding Fee and Sales Reporting, the Contractor must report the quarterly dollar value of all sales under this contract. When submitting sales reports, the Contractor must report two dollar values for each Special Item Number—

(1) The dollar value for sales to entities identified in paragraph (a) of the clause at 552.238–78, Scope of Contract (Eligible Ordering Activities)—Alternate I; and

(2) The dollar value for sales to entities identified in paragraph (d) of clause 552.238–78, Alternate I.

(d) A listing of the Federal Supply Schedule contracts for the products and services available for disaster recovery purchasing is accessible in GSA's Schedules e-Library at Web site *http://www.gsaelibrary.gsa.gov*. Click on the link, ''Disaster Recovery Purchasing, State and Local.'' The participating Contractors and the products and services available for disaster recovery purchasing will be labeled with the Disaster Recovery Purchasing icon.

(End of clause)

[72 FR 4654, Feb. 1, 2007]

552.239–70 Information Technology Security Plan and Security Authorization.

As prescribed in 539.7002(a), insert the following provision:

INFORMATION TECHNOLOGY SECURITY PLAN AND SECURITY AUTHORIZATION (JUN 2011)

All offers/bids submitted in response to this solicitation must address the approach for completing the security plan and certification and security authorization requirements as required by the clause at 552.239–71, Security Requirements for Unclassified Information Technology Resources.

(End of provision)

[76 FR 34888, June 15, 2011]

552.239–71 Security Requirements for Unclassified Information Technology Resources.

As prescribed in 539.7002(b), insert the following clause:

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2011)

(a) *General.* The Contractor shall be responsible for information technology (IT) security, based on General Services Administration (GSA) risk assessments, for all systems connected to a GSA network or operated by the Contractor for GSA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to GSA's information that directly supports the mission of GSA, as indicated by GSA. The term information technology, as used in this clause, means any equipment, including telecommunications equipment that is used in the automatic acquisition, storage, manipulation, management, control, display, switching, interchange, transmission, or reception of data or information. This includes major applications as defined by OMB Circular A–130. Examples of tasks that require security provisions include:

(1) Hosting of GSA e-Government sites or other IT operations;

(2) Acquisition, transmission, or analysis of data owned by GSA with significant replacement cost should the Contractors copy be corrupted;

(3) Access to GSA major applications at a level beyond that granted the general public; e.g., bypassing a firewall; and

(4) Any new information technology systems acquired for operations within the GSA must comply with the requirements of HSPD–12 and OMB M–11–11. Usage of the credentials must be implemented in accordance with OMB policy and NIST guidelines (e.g., NIST SP 800–116). The system must operate within the GSA's access management environment. Exceptions must be requested in